(Preprint) AAS 16-115

ORION GN&C FAULT MANAGEMENT SYSTEM VERIFICATION: SCOPE AND METHODOLOGY

Denise Brown[*], David Weiler[†], and Ronald Flanary[‡]

In order to ensure long-term ability to meet mission goals and to provide for the safety of the public, ground personnel, and any crew members, nearly all spacecraft include a fault management (FM) system. For a manned vehicle such as Orion, the safety of the crew is of paramount importance. The goal of the Orion Guidance, Navigation and Control (GN&C) fault management system is to detect, isolate, and respond to faults before they can result in harm to the human crew or loss of the spacecraft. Verification of fault management/fault protection capability is challenging due to the large number of possible faults in a complex spacecraft, the inherent unpredictability of faults, the complexity of interactions among the various spacecraft components, and the inability to easily quantify human reactions to failure scenarios. The Orion GN&C Fault Detection, Isolation, and Recovery (FDIR) team has developed a methodology for bounding the scope of FM system verification while ensuring sufficient coverage of the failure space and providing high confidence that the fault management system meets all safety requirements. The methodology utilizes a swarm search algorithm to identify failure cases that can result in catastrophic loss of the crew or the vehicle and rare event sequential Monte Carlo to verify safety and FDIR performance requirements.

INTRODUCTION

The Orion spacecraft is NASA's next generation manned spacecraft. Its proposed missions and destinations include the unmanned test flights to lunar orbit and manned flights to the moon, Mars, or near-Earth and Trojan asteroids. The Orion spacecraft is arguably the most advanced, complicated spacecraft ever designed, with the ability to operate under the control of on-board automated systems or through manual inputs from a human crew. The Orion GN&C system is designed to fly the spacecraft successfully through all phases of its unmanned test missions and through all or part of future manned missions. The system is also designed to protect against catastrophic hazards resulting from failures of GN&C components.

A hazard is a condition, state, event, or activity which has the potential to cause harm.[1] Catastrophic hazards are hazards that can result in loss of life or permanently disabling injury, loss of vehicle prior to completing its mission, or loss of essential flight/ground assets.[1] Hazards resulting from Orion GN&C faults are captured in the Orion GN&C subsystem hazard report, MPCV-FLT-0015.[2] Verification of the Orion GN&C FDIR is grouped by hazard.

In order to protect for catastrophic hazards and increase the chances of mission success, Orion includes redundant systems and automated fault detection, isolation and recovery (FDIR) software

[*]Odyssey Space Research, 1120 NASA Pkwy E. Suite 505, Houston TX, 77058.
[†]Orion GN&C FDIR Mode Team Lead, NASA, postal address.
[‡]Orion GN&C FDIR Mode Team Lead, Odyssey Space Research, 1120 NASA Pkwy E. Suite 505, Houston TX, 77058.

to detect and respond to vehicle failures. All Orion subsystems have some level of FDIR, but this paper focuses solely on the GN&C subsystem FDIR. GN&C subsystem FDIR is substantially more complicated than most FDIR on Orion, and its verification necessitates analysis of closed-loop vehicle performance in the presence of failures.

Here we will pause to define some terms commonly used in this paper. A *fault* is anything that causes a hardware component or software to perform in an unintended or unanticipated manner. A *failure* is the inability of a component or a system to perform its intended (or required) function(s). A failure is the result of one or more faults. A *hazard* is the consequence of a failure. The *time to effect* for a fault is the from fault occurrence to manifestation of the worst-case failure effect (i.e. the resulting hazard). For example, a fault in an IMU that causes that IMU to output erroneous data can result in erroneous thruster commands sent to the propulsion system. This can result in loss of control of the vehicle. In this scenario, the fault is the underlying cause of the IMU erroneous data, the IMU is failed, and the hazard is loss of control of the vehicle. The time to effect is the time between when the fault occurred and when control of the vehicle was lost. Often, the underlying fault is unknown; only its effects are seen.

Verification of the Orion GN&C FDIR is intended to demonstrate that the FDIR as designed and implemented is capable of preventing catastrophic hazards in the presence of a single fault within the GN&C subsystem or within some other subsystem that directly impacts vehicle GN&C, such as the propulsion system. Given the complexity of the Orion GN&C subsystem, the large number of possible faults to be considered, and the complex interactions within the spacecraft and between the vehicle and its operating environments, the scope of FDIR performance analysis is nearly infinite. Therefore, some means of bounding the scope while still achieving high confidence in results is necessary in order to perform verification of the GN&C FDIR within a reasonable budget and time.

The Orion FDIR mode team has developed a methodology for verifying the Orion GN&C FDIR that meets these criteria. The methodology relies upon metaheuristics in order to effectively sample the problem space and identify faults that can have catastrophic results, and then applies rare event sequential Monte Carlo techniques to verify that the Orion GN&C FDIR provides adequate protection for the catastrophic failure cases identified. The search of the sample space is critical for identifying which faults (type, magnitude, direction if applicable, time of fault) can result in loss of the crew or the vehicle and the time to effect associated with those faults. Faults that do not result in loss of the vehicle or the crew, or in loss of the mission, do not require FDIR capabilities, and faults with a long time constant do not require automated FDIR with a fast response, but may instead by resolved by the crew and/or ground operators. Identification of faults that must be handled by the on-board vehicle defines the scope and needed capabilities of the GN&C FDIR, and can also be used to tune FDIR algorithm parameters and thresholds.

The methodology allows the Orion GN&C FDIR team to focus design, analysis and verification efforts on the critical areas of the problem space.

BACKGROUND

Spacecraft fault management system analysis typically is static and probabilistic in nature. Methods such as failure modes and effects analysis (FMEAs), fault trees, and probabilistic risk assessment are common approaches.[3] However, none of these approaches are well suited to the dynamic nature of guidance, navigation and control system faults and their propagation through the spacecraft or to verification that the GN&C FDIR algorithms are sufficient to protect against GN&C subsys-

tem faults. GN&C subsystem faults predominantly affect closed-loop spacecraft performance, and unlike many other subsystem failures, the time to effect for each fault varies widely depending on the flight phase, vehicle dynamics, and multiple other factors. A fault that is benign under one set of conditions may be catastrophic under another set of conditions. The complexity of spacecraft GN&C also makes it difficult to apply standard fault management system analysis because it very difficult to predict how a fault will impact the GN&C algorithms and the overall spacecraft performance.

It is important to note that for most spacecraft, very little is known about how faults impact vehicle performance, or about how other vehicle parameters can make what might have been a benign or critical failure turn catastrophic. Fault management engineers must assume that there will be unexpected behaviors.[3] Vendors provide limited information on how failures manifest in their components, but this information is usually vague and along the lines of "erroneous data". It is not clear how that data will propagate through a complex spacecraft system and impact vehicle performance, and while knowledge of the system design and engineering judgement can provide some insight, there are often many unknown interactions and effects that result in unexpected behavior. This makes it very difficult to know which combinations of failure parameters and other vehicle and environment parameters result in catastrophic failure cases.

Due to these factors, instead of performing static, probabilistic analysis of GN&C subsystem faults and their impacts, it makes more sense to do dynamic simulation of the spacecraft response to GN&C subsystem faults, both with and without the FDIR algorithms running in the loop. Fortunately, it is common practice to build and utilize full 6 degree of freedom simulation of spacecraft for nominal GN&C subsystem analysis, and these simulations can be leveraged for GN&C subsystem fault management system analysis.

Characterization of the failure space is necessary to understand which faults have catastrophic results and what the time to effect of those failures is. The time to effect is the time between when the failure occurs and the manifestation of the catastrophic result. Each GN&C subsystem fault does not have a single time to effect associated with it; it has many times to effect depending on when during flight the fault occurs, the fault magnitude or other defining characteristics, and, in most cases, on other factors such as the vehicle mass properties or the current environment. Thus the time to effect for each fault category can best be described by a statistical distribution, and any individual occurrence of that fault is drawn from that distribution.

Identification of the faults that can result in catastrophic hazards and estimation of the statistical distributions describing the time to effect for those faults would require a nearly infinite number of runs if the search was conducted using standard Monte Carlo techniques to cover the search space. The number of variables to be dispersed is in the thousands: the type of fault, the fault parameters, the time of the fault, and all of the typical vehicle parameters such as mass properties, sensor characteristics, effector performance parameters, vehicle aerodynamic parameters (during ascent or entry), and more. Using a Latin hypercube or similar methodical search is not feasible, nor is a methodical sensitivity analysis: there are too many parameters and interactions that could be important, and too little is known in advance to perform a directed search. Also, because of the uncertain knowledge of how faults will manifest and what their impact will be, a methodical or directed search has a high likelihood of missing important parts of the search space.

Swarm optimization algorithms have proven effective at searching large, complex problem spaces in multiple fields.[4] More recent adaptations have been developed that specialize in the search for

multiple optima.[5,6,7] These multi-optima swarm optimization algorithms would seem to be well-suited to identifying which spacecraft faults can result in catastrophic hazards. The problem space is large, unknown, and has multiple "optima". The Orion FDIR team will be employing a multi-optima swarm optimization algorithm to search the failure space.

Particle swarm techniques have been successfully applied to search for failures in power systems.[8,9] In the latter case, the authors were able to identify failure states with 1/7 of the number of runs required to identify the same states using traditional Monte Carlo methods.[9]

It should be noted that swarm optimization algorithms are not guaranteed to find all of the possible combinations of faults and other spacecraft parameters that will result in a catastrophic failure. However, these algorithms can identify more of the catastrophic failure cases and the associated times to effect in a shorter time than manual search techniques, sensitivity analysis, or the standard Monte Carlo techniques typically employed by GN&C analysts.

Once the fault scenarios that can result in catastrophic hazards are identified, the driving cases can be found using engineering judgement. These cases can be used to direct the next step of the GN&C FDIR verification, which is to demonstrate that the GN&C FDIR algorithms are capable of protecting against the identified faults. It should be noted that the analysis of which failures can result in catastrophic hazards is performed without any GN&C FDIR algorithms running; it is intended to identify what those algorithms must provide protection for, and, if done early enough, can guide the FDIR design. Understanding of the failure space is also necessary to perform verification of the fault management system algorithms and architecture.

Orion is required to provide a minimum of one fault tolerance to catastrophic hazards, and to provide some level of control for critical hazards in order to improve the chance of mission success. There are no metrics associated with these requirements, but 100% protection for all faults is not possible for many reasons, not least of which is the lack of ability to predict all of the ways in which a vehicle can fail. However, in a well-designed spacecraft, the probability of failing a requirement - in this case, of having a catastrophic failure that is not mitigated by the vehicle fault management system - will be extremely rare. In fact, it is desirable that this probability be as low as possible. NASA standards dictate that the probability of a catastrophic hazard must be less than $1e{-}6$ in order to consider that hazard adequately mitigated.[1]

Table 1. Number of Required Runs Using Standard Monte Carlo Analysis for Varying Probabilities of Catastrophic Failure

Probability of Catastrophic Failure (%)	Confidence (%)	Number of Runs
$1e{-}4$	50	6931
$1e{-}4$	90	23025
$1e{-}4$	95	29956
$1e{-}6$	50	693147
$1e{-}6$	90	2302584
$1e{-}6$	95	2995731

Using standard Monte Carlo techniques, it would require 693,147 runs to show that the probability of catastrophic failure was less than 99.999999% with 50% confidence if no runs were allowed to result in catastrophic failure.[10] It would require 2,302,584 runs if the confidence were increased to 90%. As the probability of catastrophic failure decreases or the desired confidence increases, the number of runs increases, as shown in Table 1.

Rare event sequential Monte Carlo (SMC) analysis can be used to establish the probability of rare events using far fewer runs than a straight Monte Carlo approach.[11] This makes rare event SMC well-suited to many kinds of fault management analysis because in general the probability of any failure occurring are considered to be small, and rare event SMC is designed to efficiently seek out rare occurrences. The Orion FDIR team will employ rare event sequential Monte Carlo analysis for verification of the Orion GN&C FDIR algorithms and architecture.

The authors have employed rare event sequential Monte Carlo to determine the probability of meeting fault management system requirements for FM systems modeled as discrete dynamic Bayesian networks. This work demonstrated that rare event SMC was effective at determining the probability of meeting fault management system requirements with approximately 1/10th of the number of runs required using traditional Monte Carlo.[12]

ORION GN&C FAULT MANAGEMENT SYSTEM ANALYSIS SETUP

Setting up the Orion GN&C FM system analysis is not a trivial task, and there are multiple aspects of the analysis that require careful planning. In order to make the analysis as efficient as possible, concerns such as simulation run speed, data storage, memory usage, and processing loads must be addressed. Simulation of faults also requires a means of injecting faults into a simulation, and efficient, data-driven fault injection is a key factor for successful FM system analysis.

Orion GN&C Subsystem Overview

The Orion GN&C FDIR scope includes all failures of GN&C system components, such as navigation sensors and GN&C algorithms, as well as failure of non-GN&C subsystem components such as the propulsion system, that impact the vehicle's ability to maintain control and fly its desired trajectory. The Orion program requires a minimum of single fault tolerance to catastrophic failures. Catastrophic failures are defined as failures that can result in loss of human life or serious injury, loss of the spacecraft, and/or loss of major flight assets such as ground facilities. It is also desirable to provide some minimum level of protection for critical failures that can result in premature mission termination, and although these are not the focus of this paper, they are considered by the Orion GNC&C FDIR team.

The Orion GN&C is responsible for controlling the vehicle's trajectory and attitude during all phases of free flight following separation from the launch vehicle. The vehicle uses data from multiple redundant navigation sensors in redundant extended Kalman filters (EKFs) to determine its inertial position and attitude throughout the mission. The vehicle also includes a backup optical navigation system, but this system will not be utilized unless the primary navigation fails.

Orion employs a variety of targeting, guidance, and pointing algorithms to calculate commands for vehicle trajectory and attitude maneuvers. Some of these algorithms use data from the EKFs, while others directly use data from the navigation sensors, such as IMU accelerations. Some of the Orion controller algorithms also use navigation sensor data that has not passed through the vehicle EKFs. Therefore the Orion GN&C FDIR must consider sensor failures that impact the navigation filter solutions as well as sensor failures that impact data used directly within guidance and control algorithms.

Failures within the Orion propulsion systems can also adversely impact the vehicle's ability to maintain control and fall under the umbrella of Orion GN&C FDIR. There is limited FDIR within the propulsion systems in the form of monitoring of temperature and pressure sensors, but the Orion

GN&C subsystem also monitors the health of the service module main engine thrust vector controllers and the overall control system performance while in Earth and lunar orbit in order to detect off-nominal propulsion system performance that could result in incorrect trajectory maneuvers or incorrect attitude. The Orion GN&C subsystem is also responsible for detecting failures of the service module solar array actuators.

Therefore Orion GN&C FDIR verification is concerned with failures of navigation sensors and with failures of several of the vehicle effectors. Unlike many other subsystems, GN&C FDIR is concerned not only with loss of data from a sensor or loss of output from an effector, which are easy to detect and respond to by switching to a redundant component, but with erroneous output. Erroneous output failures are harder to detect and isolate, but these can have catastrophic results, and GN&C FDIR performance analysis and verification focuses primarily on erroneous data failures.

Orion GN&C Subsystem Faults

There are literally thousands of different faults that can occur within the GN&C subsystem or within components and subsystems that directly interact with the GN&C. In order to make the GN&C FM system analysis tractable, the Orion GN&C FDIR team has grouped faults by failure signature. A *failure signature* is particular manifestation of a fault in the output of a component. An example of a failure signature is a bias shift in the IMU gyro output. There are many different faults that can cause a gyro bias shift, such as failure of a voltage regulator, mechanical damage to an electrical component due to excessive vibration levels during ascent, or inadvertent memory modification of some part of the IMU RAM that processes gyro data. From a GN&C performance perspective, the underlying fault is of less interest than the signature of how that fault manifests in the component output. The Orion GN&C FDIR mode team has identified over 150 different failure signature categories that can negatively impact GN&C performance. Faults are categorized by the component that fails (e.g. IMU, star tracker, RCS jet) and the failure signature (e.g. loss of data, bias shift, failure to activate, etc.). The failure signature categories were compiled based on Failure Modes and Effects Analyses (FMEAs) provided by the hardware vendors, experience with similar hardware on other spacecraft, and historical data. The team did a thorough search of NASA's anomaly databases for the Space Shuttle, ISS, the ISS visiting vehicles (ATV, HTV, Soyuz, etc.) and researched published literature on spacecraft failures.

Within each failure signature category, the parameters describing the failure can vary. For example, a slow drift bias in an accelerometer might have a drift rate anywhere between 100 micro-gs per day or 1 micro-g per hour. Faults that result in excessive noise must be described by the type of noise (white, green, pink, etc.) and the statistical characteristics of that noise. When available, failure signature parameter dispersions were taken from historical and vendor data. When no data was available (which was the majority of the time), engineering judgement was used to establish boundaries on failure signature parameters. In some cases, failure signatures are completely random within a given bound, such as the case of contamination of star tracker optics, in which a star tracker may output any possible 3-dimensional rotation dependent on the contamination pattern on the optics and the sensor internal parameters and algorithms.

Orion GN&C Simulation

The Orion GN&C team uses a high fidelity 6 degree of freedom vehicle simulation called Antares coupled with a simulation of the GN&C flight software to perform GN&C subsystem analysis.

Antares includes models of the Orion GN&C hardware, and it models the environment and vehicle dynamics. The GN&C software simulation contains all of the GN&C algorithms and simple emulations of other flight software components that provide data needed by GN&C.

These simulations have a great deal of heritage, they are incredibly complex, and they are not optimized for speed. They were also not designed with FDIR analysis in mind and their ability to inject failures was limited. To overcome that limitation, the FDIR team worked with the Antares design team and software engineers to develop a generic fault injection architecture that allows any failure from a library of faults to be injected on any variable within the Antares simulation at any time based on one or more conditions within the simulation. The generic fault injection model is completely data driven, with the fault types, fault parameters, and fault injection triggers specified in XML files. The fault injection model is incredibly powerful and it gives the GN&C FDIR team flexibility to model all of the failure signatures and fault injection conditions needed for the GN&C FM system analysis.

The Orion EM-1 mission is 25 days. Speeds of no greater than 10 to 15 times real time can be expected from the GN&C simulation tools, which means a full end-to-end simulation takes approximately 1.5 to 2.5 days to run. In order to reduce simulation run time as much as possible the GN&C FDIR team has:

- Identified simulation checkpoints for scenarios of interest that result in the shortest feasible simulation run times for FM system analysis
- Created efficient, minimalistic data logging
- Created routines to terminate a simulation when a catastrophic failure occurs
- Identified models that can be turned off or whose efficiency can be increased through changing data settings without compromising the fidelity of the simulation

An example of this latter case is the simulation gravity model. Normally, the gravity model is a 10x10 EGM96 model and it is one of the most inefficient simulation models. During cis-lunar transit, this model can be set to run a lower fidelity gravity field without compromising simulation results.

The GN&C flight software simulation is somewhat rigid since it emulates the actual vehicle flight software, but it is possible to use the crew and ground commanding capabilities within the GN&C flight software to properly configure the GN&C FDIR algorithms for the FM system analysis. When performing the search of the failure space, the FDIR algorithms are all effectively disabled.

The GN&C simulations natively support single runs and traditional Monte Carlo analysis. The simulations do not support advanced Monte Carlo techniques or optimization routines. Those must be developed independently.

Catastrophic Failure Criteria

In order to assess when a catastrophic failure has occurred, the Orion GN&C FDIR team used the vehicle requirements, engineering judgement, and experience with other spacecraft to generate a set of quantifiable criteria that can be automatically checked during simulation runs or through post processing of logged data.

For the Orion vehicle, catastrophic failures of the GN&C subsystem fall into five categories:

- Failure to perform critical events
- Premature depletion of consumables
- Excessive crew acceleration loads
- Exceeding vehicle thermal and structural limits
- Loss of control of the vehicle

Critical events consist of things like separation from the launch vehicle and deployment of parachutes during entry. Failure to perform these events will result in catastrophic failure and loss of or serious injury to the vehicle crew, or loss of the vehicle.

Premature depletion of consumables such as oxygen or fuel can result in loss of the life of any crew members on board the vehicle, or in inability to return the crew safely to earth.

NASA defines maximum sustained and transient translational and rotational acceleration limits to which humans can be exposed.[13] Many of the limits date back to the Apollo program. Exceeding these limits endangers the lives of the crew members.

Exceeding vehicle structural and thermal limits, especially during entry, can result in breakup of the vehicle and loss of the crew. Many of the Orion GN&C subsystem requirements are intended to ensure the vehicle remains within acceptable structural and thermal limits.

The final category, loss of control of the vehicle, encompasses control margins and vehicle stability as well as more common sense concepts, such as maintaining a minimum altitude above the lunar surface and landing the vehicle within a specific distance of the target landing point in order to ensure rescue teams can reach the crew quickly.

Table 2. Catastrophic Failure Criteria

Category	**Condition**
Critical Event	Drogue chutes deployed within acceptable altitude limits
Consumable Depletion	Propellant sufficient to complete landing
Acceleration Limits	Sustained rotational acceleration under main parachutes under maximum limits
Thermal/Structural Limits	Heat shield forward attitude maintained
Vehicle Control	Orion lands within X km of targeted landing site

Violation of any criteria in any of these categories is considered a catastrophic hazard. The criteria limits and the criteria themselves vary by flight phase. Table 2 shows example catastrophic failure criteria for entry.

When possible, checking for the occurrence of catastrophic failure criteria is performed during simulation run time. Post-processing is reserved for checking conditions that require significant time history data and for accumulating statistics across multiple runs. The post-processing scripts are Python scripts designed to run in parallel.

Swarm Search to Identify Faults that Result in Catastrophic Failure

To effectively search the fault space, a multi-optima swarm search algorithm will be employed. The use of a multi-optima search method is necessary because we are not attempting to find an optimal solution; we are attempting to perform a thorough search of the failure space to identify all GN&C subsystem faults that can result in a catastrophic hazard.

The GN&C FDIR team has not yet selected which multi-optima swarm algorithm will be used, but based on results in the literature and the nature of the failure space search problem, the locust swarm[6] and Waves of Swarm Particle (WoSP)[5] are the preferred algorithms. Chen and Montgomery discuss efficient initial condition selection for the algorithms and demonstrate the effectiveness of their initial condition selection approach on multi-modal problems.[14]

Each swarm particle will require a single execution of the GN&C simulation during each algorithm step. The fitness of each particle is a simple function based on whether or not a catastrophic failure occurs, as shown in Equation 1.

$$F_i = \begin{cases} 0 & \text{if fault } i \text{ results in catastrophic failure} \\ 1 & \text{otherwise} \end{cases} \tag{1}$$

We want to minimize the fitness function, F, so a particle in which a catastrophic failure occurs will have a fitness of zero, while a particle in which a catastrophic failure does not occur will have a fitness of 1.

Tuning particle swarm optimization algorithms is one of the major difficulties associated with these approaches.[15,9] It is necessary to balance exploration and exploitation, and some work will be necessary to tune the swarm algorithm for the FDIR failure search problem. The number of particles used and the algorithm parameters will be tuned to achieve the goals of the search. Some trial and error will likely be necessary to identify effective tuning.

The search of the failure space will provide a wealth of information, including

- which faults result in catastrophic failures,
- the type of catastrophic failure(s) that result from different types of faults,
- the time to criticality distribution associated with the different types of faults,
- identification of other factors that have a significant impact on vehicle behavior in the presence of failures,
- and a general understanding of the effect of GN&C subsystem faults on vehicle performance.

One additional goal of the failure space search is to determine which GN&C subsystem faults result in which catastrophic hazards. Hazards resulting from Orion GN&C faults are captured in the Orion GN&C subsystem hazard report, MPCV-FLT-0015.[2] As mentioned previously, verification of the Orion GN&C FDIR is grouped by hazard, and the probability of any given hazard occurring must be less than $1\mathrm{e}{-6}$.

Orion GN&C FDIR Verification

The swarm search will determine which faults result in catastrophic failure and the time to effect for those faults. The search may also identify other factors, such as space craft mass properties, that have a significant impact on how faults affect vehicle performance. The search cannot be guaranteed to find all fault scenarios that result in catastrophic failure, but it can identify many of them. These scenarios will be the starting point for the GN&C FDIR software verification.

The goal of GN&C FDIR software verification is to demonstrate that the GN&C FDIR algorithms and their implementation meet safety and FDIR performance requirements, namely that they detect, isolate, and recover from failures before a catastrophic failure occurs. In other words, the time it takes the FDIR software to detect a fault, isolate its source, and recover from it must be less than the time to effect for any given fault.

Sequential Monte Carlo is a type of particle filter, and each SMC sample is referred to as a particle. Each particle is a successive series of GN&C simulation executions, the evolution of which is governed by the SMC algorithms. For GN&C FDIR verification, a pure mutation method will be used to evolve the particles.

At each SMC step, the particles will be randomly mutated and evaluated for fitness. Samples that are a better fit are weighed more heavily than samples that are less fit. Each step in the SMC sequence thus requires

- A method for mutating the particles
- A method for evaluating fitness

The mutation approach must be chosen to mutate the particles to effectively explore the sample space and improve the overall fitness of the population. A Metropolis-Hastings random walk method[16] will be utilized, in which the fault parameters and fault injection time will be changed randomly according to a random walk algorithm and the simulation results will be re-evaluated with the new values. This is done at each step of the SMC sequence.

The sequence of fitness functions (weight and cost) will be designed to evaluate the fitness relative to the target probability distribution we want to sample from at each step in the sequence. Therefore, to define fitness functions a sequence of target distributions are needed. Typically the sequence of target distributions is constructed so that the initial distribution is known and easy to sample from, the final distribution is the specific distribution we want to sample from, and the intermediate kernels transition smoothly from the initial distribution to the final distribution.[17]

The initial samples for each particle will be the GN&C simulation results for initial conditions randomly selected from the results of the failure space search. The target distributions will be constructed from the joint distribution of the simulation initial conditions at each SMC step multiplied by a function that indicates whether those simulation initial conditions met given conditions. In the final distribution, these conditions are the specific requirements the system should be meeting, while in the initial distribution, any conditions are accepted. During the transition from the initial to the final distribution, the conditions are a step-wise tightening of the requirements until the desired values are reached.

For Orion GN&C FDIR verification, at the first SMC step, the fitness criteria is such that any result is acceptable, including a run that ends in catastrophic failure. At the next step, the fitness

criteria will be that the probability of catastrophic failure will be less than 90%, then 80% for the next step, and so on, until the final condition is reached, which is that the probability of catastrophic failure with the FDIR algorithms in the loop is less than $1e{-}6$.

Algorithm 1 Sequential Monte Carlo Algorithm

1: For each particle, do an initial execution of the simulation with a random set of catastrophic failure cases from the swarm search
2: **for** steps $i = 2, ..., N$ **do**
3: Randomly mutate fault parameters and injection time
4: Execute the simulation with the new initial conditions
5: Determine whether each particle meets the current fitness criteria
6: Compute particle weights based on whether or not the fitness criteria are met
7: Keep particles that have weight $>$ minimum allowed weight
8: **end for**

Algorithm 1 show the steps for the sequential Monte Carlo analysis. The SMC analysis can be done in one of two ways: a separate SMC analysis can be performed for each type of fault that results in a catastrophic hazard, such as IMU accelerometer bias shifts during entry or contamination of star tracker optics just prior to large orbit maneuvers, or the analysis can be set up to search across all identified catastrophic failure cases simultaneously.

It is not necessary that the probability of each fault resulting in a catastrophic failure is less than $1e{-}6$; it is only necessary that the overall probability of each individual hazard is less than $1e{-}6$.[1] Suppose there are N different possible Orion GN&C subsystem faults that can result in catastrophic hazard X. According to basic probability theory, the probability of any of the N faults resulting in catastrophic hazard X is given by equation 2,[18] where $P(C_i)$ is the probability that fault i will result in hazard X.

$$P(C_1 i \vee C_2 \vee ... \vee C_N) = \sum_{i=0}^{N} P(C_i) \tag{2}$$

It isn't safe to assume the faults are all independent - they may have the same underlying cause - but the faults can be assumed to be mutually exclusive since only one fault must be considered at any given time to meet a single fault tolerant requirement. The probability of individual faults resulting in a catastrophic failure, $P(C_i)$ depends on the performance the GN&C FDIR algorithms.

Therefore, analysis could be performed to calculate each $P(C_i)$ for a given hazard X, then those individual probabilities could be summed to calculate the overall probability of hazard X. If that probability is greater than the allowed probability of $1e{-}6$, then it indicates there is a deficiency in the GN&C FDIR algorithms and architecture that protect for that hazard, and it will be necessary to redesign some portion of that FDIR. In this case, there would be a separate SMC analysis performed for each fault i.

It is also possible to perform analysis that covers all causes of a single hazard at one time. In this case, the faults injected during the analysis would be just another random variable to be mutated. Although this is slightly more difficult to set up than running individual analyses for each fault, it should be more efficient, and this is the approach the GN&C FDIR team will take.

There is no standard formula for the number of SMC steps required to reach the final distribution, nor is there a standard formula for the number of particles needed. These values must be tuned

through intuition and testing. Initially, the SMC will be set to use 50 particles executed for 20 steps. These values will be modified as needed over the course of the GN&C FDIR verification.

CONCLUSION

The use of metaheuristics can improve the efficiency and effectiveness of fault management system analysis. Particle swarm search algorithms can be used to determine which faults result in catastrophic hazard and to understand how those faults propagate through the vehicle. Such methods provide a more thorough exploration of the failure space with fewer runs than manual searches based on engineering judgement or sensitivity analysis examining the thousands of variables that can impact vehicle performance in the presence of faults. Rare event sequential Monte Carlo methods provide an efficient and effective means of verifying fault detection, isolation, and recovery algorithms and architecture with fewer runs than traditional Monte Carlo approaches.

REFERENCES

[1] "MPCV 70038 MPCV Program Hazard Analysis Methodology," February 2014.

[2] "Loss of Vehicle Control," tech. rep., MPCV-FLT-015, MPCV Program Hazard Report, 2015.

[3] S. Johnson, T. Gormley, S. Kessler, C. Mott, A. Patterson-Hine, K. Reichard, and P. Scandura, Jr., eds., *System Health Management with Aerospace Applications*. The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, UK: John Wiley & Sons Ltd, 1st ed., 2011.

[4] R. Poli, J. Kennedy, and T. Blackwell, "Particle Swarm Optimization – An Overview," Swarm Intelligence, 2007.

[5] T. Hendtlass, "WoSP: a multi-optima particle swarm algorithm," *The 2005 IEEE Congress on Evolutionary Computation*, IEEE, 2005, pp. 727–734.

[6] S. Chen, "Locust Swarms - A new multi-optima search technique," *The 2009 IEEE Congress on Evolutionary Computation*, IEEE, 2009, pp. 1745–1752.

[7] A. Rohler and S. Chen, "Multi-swarm hybrid for multi-modal optimization," *The 2012 IEEE Congress on Evolutionary Computation*, IEEE, 2012, pp. 1–8.

[8] J. Mitra and X. Xu, "Composite system reliability analysis using particle swarm optimization," *International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, IEEE, 2010, pp. 548–552.

[9] M. Benidris, S. Elsaiah, and J. Mitra, "Composite System Reliability Assessment Using Dynamically Directed Particle Swarm Optimization," *North American Power Symposium (NAPS), 2013*, IEEE, 2013, pp. 1–6.

[10] J. Tietz, "What does "Three Sigma" Mean? Probabilty and Statistics in the Context of Spacecraft Design," tech. rep., NASA, 2008.

[11] F. Cerou, P. Del Moral, T. Furon, and A. Guyader, "Sequential Monte Carlo for Rare Event Estimation," *Statistics and Computing*, Vol. 22, No. 3, 2012, pp. 795–808.

[12] D. Brown, A. Brown, J. Burch, and A. Lopez-Dayer, "Dynamic State-based FM Design and Analysis Tool Phase I Final Report," tech. rep., NASA Small Business Research Initiative No. NNX15CA52P, 2015.

[13] "MPCV 70024 Orion MPCV Program Human Systems Integration Requirements," January 2014.

[14] S. Chen and J. Montgomery, "Selection Strategies for Initial Positions and Initial Velocities in Multi-Optima Particle Swarms," *Proceedings of the 13th annual conference on Genetic and evolutionary computation*, ACM, 2011, pp. 53–60.

[15] M. E. H. Pedersen, *Tuning and Simplifying Heuristical Optimization*. PhD thesis, University of Southampton, January 2010.

[16] A. M. Johansen, P. Del Moral, and A. Doucet, "Sequential Monte Carlo Samplers for Rare Events," tech. rep., University of Cambridge, Department of Engineering, Trumpington, UK, 2005.

[17] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*. London, UK: Pearson, PLC, 3rd ed., 2010.

[18] R. Ott and M. Longnecker, *An Introduction to Statistical Methods and Data Analysis*. Pacific Grove, CA, USA: Duxbury Press, 5th ed., 2001.